

REMARKS

Claims 1-30 are pending.

Claims 1-30 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,363,149 (Candelore). Applicants respectfully disagree with that rejection.

Claim 1 recites a method that includes sending a first message (*e.g.*, KEY 2, SEQ+2 in FIG. 4) containing a first sequence identifier (*e.g.*, SEQ+2) and a digest of routing information that has been calculated using a first authentication key (*e.g.*, KEY 2); and subsequently sending a second message (*e.g.*, KEY 1, SEQ+1) containing a second sequence identifier (*e.g.*, SEQ+1) that is earlier in a sequence than the first sequence identifier (*e.g.*, SEQ+2) and a digest of the routing information that has been calculated using a second authentication key (*e.g.*, KEY 1).

Certain advantages of the claimed subject matter may be appreciated by referring to the exemplary network illustrated in FIG. 4 of the present application. That network includes multiple routers 12A, 12B, 12C that are adapted to process messages only if 1) the sequence number associated with the message is greater than the sequence number associated with the most recent message processed; and 2) the authentication key associated with the message is the key that is expected by the receiving router. In the illustrated network, an authentication key rollover has successfully been implemented in routers 12A and 12B (to KEY 2), but not in router 12C (remains at KEY1). Router 12A is shown transmitting a routing message twice, including first routing message (KEY 2, SEQ+2) using the new key (KEY 2) and second routing message (KEY 1, SEQ+1) using the old key (KEY 1).

Since the key rollover was not completed in router 12C, that router expects KEY 1. Accordingly, when that router 12C receives the first message (including KEY 2), the router 12C ignores the first message and does not expend processing effort on that first message. Subsequently, when the router 12C receives the second message (KEY 1, SEQ+1), the router 12C accepts and processes that second message because the sequence number (N+1) of the second message is greater than the sequence number (N) of the previously processed message

and because the key (KEY 1) of the second message was the same key that was expected by the router 12C.

On the other hand, since the key rollover was successfully implemented in router 12B, that router 12B expects KEY 2. Accordingly, when the first message (including KEY 2) reaches the router 12B, that router 12B accepts and processes the first message because the first message includes the expected key (KEY 2) and because the sequence number of the message ($N + 2$) is greater than the sequence number (N) of the previously processed message. When the second message reaches the router 12B, that router 12B does not process the second message because the sequence number ($N + 1$) of the second message is less than the sequence number ($N + 2$) of the routing message that was most recently accepted and processed by that router 12B.

In view of the foregoing comments, it can be appreciated that, implementing the method recited in claim 1 can help ensure that every router (*e.g.*, 12B, 12C), in a network where authentication key rollover occurs, receives and efficiently processes messages that are sent by other routers. The Candelore patent simply fails to disclose or suggest the features recited in claim 1.

Instead, the Candelore patent discloses a method that includes generating a series of keys that are related to one another in such a manner that each key in the series can be used to derive previous keys in the series, but not subsequent keys in the series. (*See* FIG. 1 and box 515 in FIG. 5B) Accordingly, if a previously recorded program requires a key from a previous time period in order to be viewed, that earlier key can be derived from the current key using a one-way hash function. (*See* Abstract) The Candelore patent fails to disclose or suggest sending a first message containing a first sequence identifier and a digest of routing information that has been calculated using a first authentication key; and subsequently sending a second message containing a second sequence identifier that is earlier in a sequence than the first sequence identifier and a digest of the routing information that has been calculated using a second authentication key, as is recited in claim 1.

Claim 1 should be allowable for at least the foregoing reasons.

Claims 2-8 depend from claim 1 and, therefore, should be allowable for at least the same reasons as claim 1.

Independent claims 9, 14, 20, 25, 27 and 29 recite features that are similar to those recited in claim 1. Accordingly, those claims should be allowable for at least the same reasons discussed above with reference to claim 1.

Claims 10-13, 15-19, 21-24, 26, 28 and 30 respectively depend from allowable claims and, therefore, should be allowable for at least the same reasons as the claims from which they depend.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

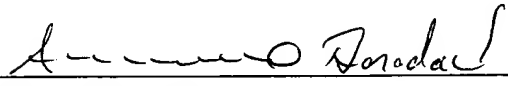
No fee is believed to be due. However, please apply any charges or credits to deposit account 06-1050.

Applicant : Jacek Szyszko
Serial No. : 09/734,834
Filed : December 11, 2000
Page : 5 of 5

Attorney's Docket No.: 10559-369001 / P10175
Assignee : Intel Corporation

Respectfully submitted,

Date: 11/10/05



Samuel Borodach
Reg. No. 38,388

Fish & Richardson P.C., Attorneys for Intel Corporation
4350 La Jolla Village Drive
Suite 500
San Diego, CA 94122
Telephone: (858) 678-5070
Facsimile: (858) 678-5099